QSC19

Qualys Security Conference Mumbai, India

Improving Defense Posture through Intelligence-based Vulnerability Management

Afzal Mohamed
Head of IT Security – Nomura India

Agenda

Challenges Related to VM

Industry and Regulatory Requirements

Intelligence based VM program

Security Automation and Orchestration

ADVERSARIES DON'T NEED MANY VULNERABILITES
ONE IS ENOUGH

Every

36 minutes

a new security vulnerability
Is identified

It takes an average of

100 days

until known security vulnerabilities
are remediated**

That is an average of*

93 unique vulnerabilities

per asset in the Financial industry

13 unique vulnerabilities

per asset in the Healthcare industry

7 unique vulnerabilities

per asset in the Technology industry

That is an average of

14,600 known

and disclosed vulnerabilities each
Year*

It takes

15 days

on average for a vulnerability to be
Exploited**

Sources: Nopsec risk report 2018* and Gartner threat report**

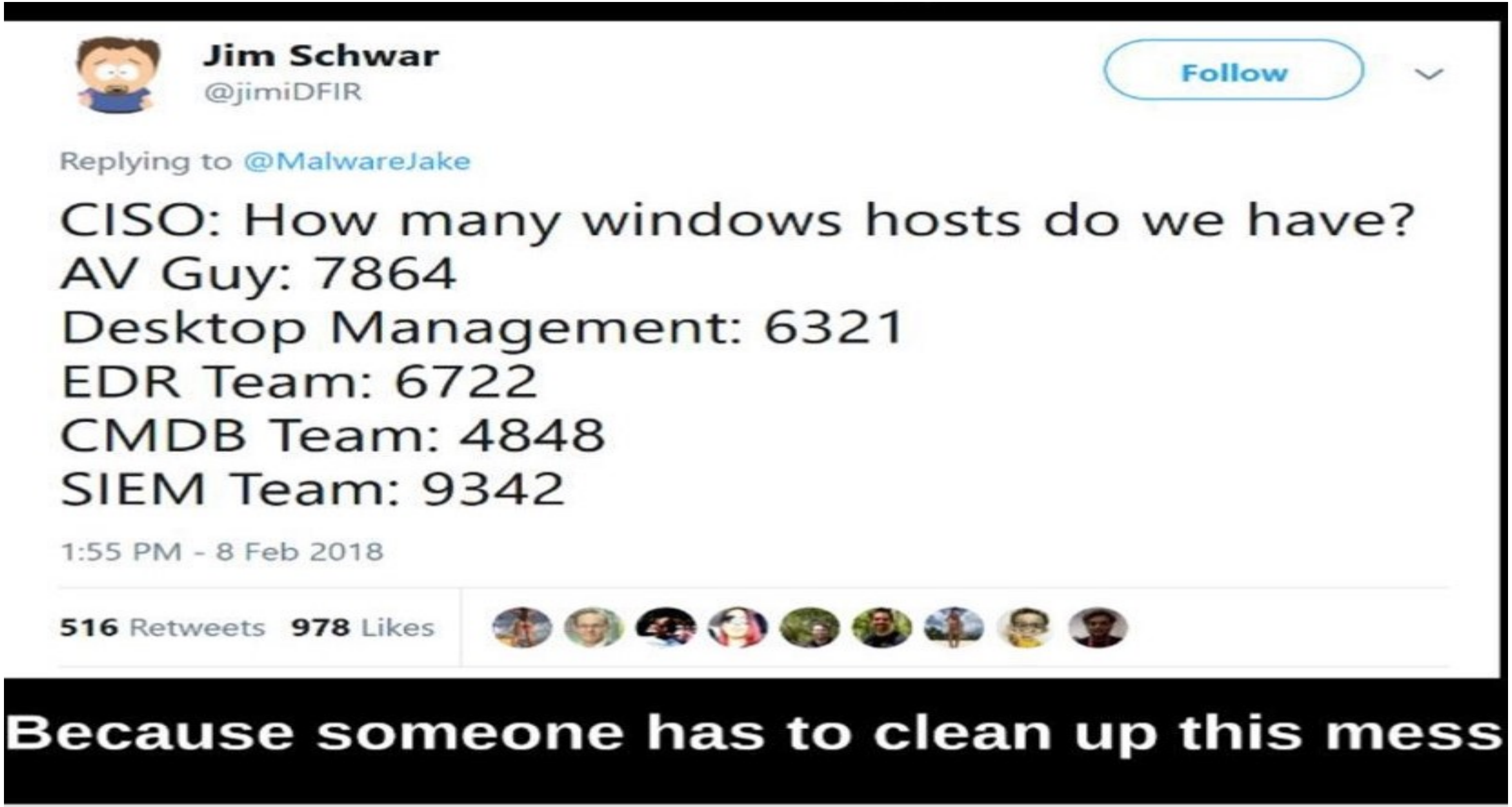
Vulnerabilities management related challenges

Recent ESG research on Cyber risk management, which involved 340 Cybersecurity professional shows;

- 43% respondents indicate that their biggest vulnerability management challenge is prioritizing which vulnerabilities to remediate. Sound familiar?
- 42% mention that their vulnerability management challenge is tracking vulnerability and patching vulnerabilities in a timely manner
- 41% of respondents indicate that their biggest vulnerability management challenge is tracking the cost and effectiveness of their vulnerability management program
- 40% of respondents indicate that their biggest vulnerability management challenge is keeping up with the volume of vulnerabilities

Source : CSOonline.com

Vulnerabilities management related challenges



Jim Schwar
@jimiDFIR

Replying to @MalwareJake

CISO: How many windows hosts do we have?
AV Guy: 7864
Desktop Management: 6321
EDR Team: 6722
CMDB Team: 4848
SIEM Team: 9342

1:55 PM - 8 Feb 2018

516 Retweets 978 Likes

Because someone has to clean up this mess

Industry and Regulatory requirements for VM

- Compliance
- Robust patching program
- Protecting Crown Jewel
- Prioritization of Threat
- Effective Remediation

Why Intelligence based VM program ?

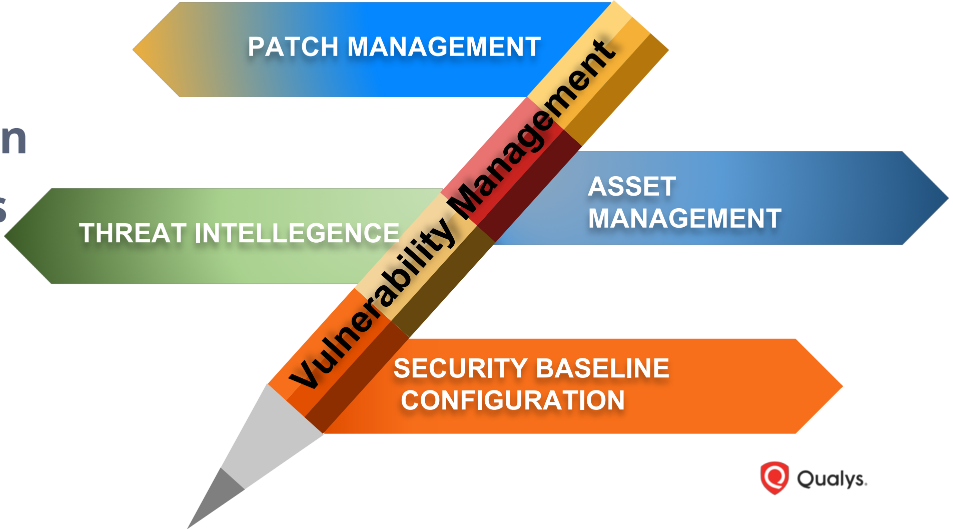
Intelligence based VM assist in timely identifying threats in your environment and help improve detection and mitigation response times.

Cyber threat Intel combined with risk based vulnerability remediation can significantly reduce the attack surface along with lateral movement.

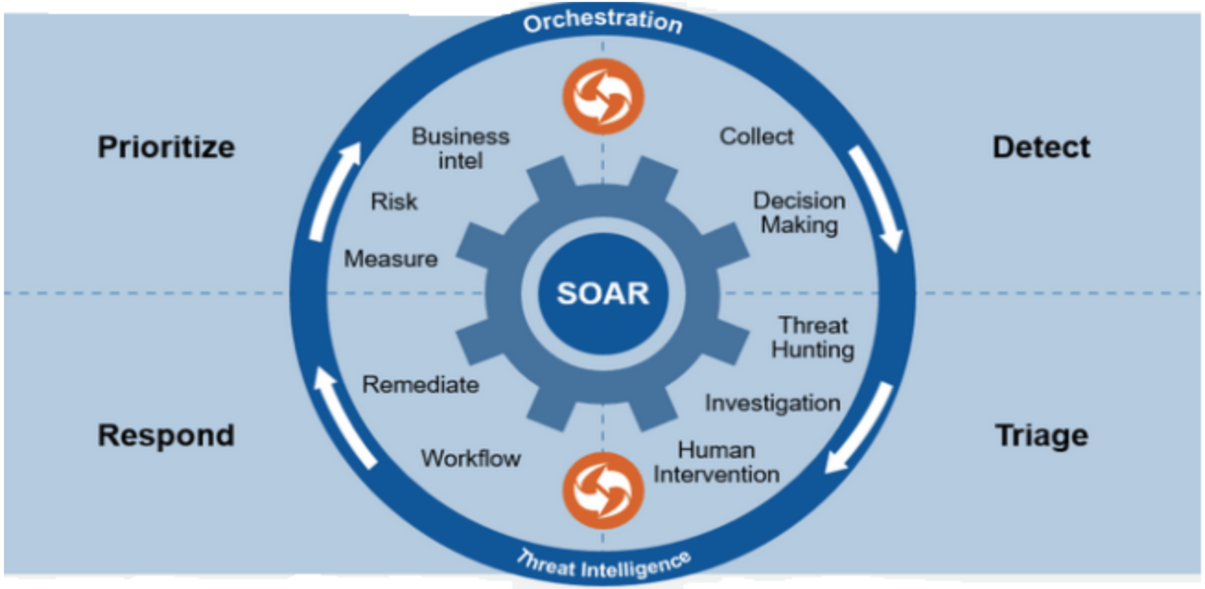
Gartner forecasts around 30 percent of organizations will adopt a risk-based approach to vulnerability management by 2022, which could help them suffer 80 percent fewer breaches.

Benefits of Intelligence based VM program;

- **Reduce effort to prioritize remediation**
- **Targets only applicable vulnerabilities**
- **Focus on Crown Jewel**
- **Effective VM program**



Security Orchestration, Automation and Response



- Prioritizing operations activities
- Formalizing triage and incident response
- Automating workflows
- Creating transparency and a common business language

Sources: Gartner

Qualys.

Key Takeaways

- Identify your old enemies - 90% of Companies get attacked with three years old vulnerabilities
- Implement a vulnerability management program that includes discovery, prioritization and then treatment
- Continuously discover, monitor, assess and prioritize risk and trust — reactively and proactively
- Effective vulnerability management can significantly lower the cost of security
- Put continuous risk visibility, decisions and ownership to business units and platform owners
- Threat Intel and Risk based remediation
- Use analytics, AI, automation and orchestration to detect faster and risk-prioritize remediation

Thank You

afzal.mohamed@nomura.com

Disclaimer: Views expressed are my personal and not those held by my firm.